UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/705,782	11/10/2003	Andrew Dellow	851963.414	4386

38106 7590 10/03/2007

SEED INTELLECTUAL PROPERTY LAW GROUP PLLC
701 FIFTH AVENUE, SUITE 5400
SEATTLE, WA 98104-7092

EXAMINER	
DEBNATH, SUMAN	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
10/03/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/705,782	DELLOW ET AL.	
	Examiner	Art Unit	
	Suman Debnath	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 are pending in this application.

2. Claims 9-10, 13, 16 and 19 are presently amended.

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office Action.

Claim Rejections - 35 USC § 103

4. Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Horne (Patent No.: 4,887,296) and further in view of Ishibashi et al. (Patent No.: US 6,728,379 B1) (hereinafter "Ishibashi") and Yokoyama et al. (Patent No.: US 6,625,147 B1) (hereinafter "Yokoyama").

5. As to claim 1, Horne discloses a semiconductor integrated circuit for decryption of broadcast signals (column 2, lines 36-44), comprising: an input interface for receipt of received encrypted broadcast signals and control data (column 2, lines 5-11 and lines 36-69; which describes decryption circuit receives encrypted signals and addressable control data), and an output interface for output of decrypted broadcast signals (column 2, lines 5-11; which describes broadcast signals being decrypted in receiving end and having necessary interface to interact with the decoder); a processing unit arranged to receive encrypted broadcast signals via the input interface (FIG. 2, column 2, lines 5-11), to decrypt the encrypted broadcast signals in accordance with control signals (column 8, lines 42-58), and to provide decrypted broadcast signals to the output

interface (column 2, lines 5-11); a first decryption circuit arranged to receive encrypted control signals from the input interface (column 2, lines 38-40 and lines 5-11); a second decryption circuit arranged to receive the common key in encrypted form from the input interface and to decrypt the common key in accordance with a secret key from a secret key store (column 4, lines 28-36); whereby the circuit is arranged such that the only route is to input the common key in encrypted form for decryption in accordance with the secret key (column 4, lines 28-36), and the only route to providing the control signals to the processing unit is to input them in encrypted form (FIG. 4, column 4, lines 34-36 and column 8, lines 42-58).

Horne doesn't explicitly disclose placing common key in the common key store and decrypting the control signals in accordance with the common key. However, Ishibashi discloses placing common key in the common key store (column 6, lines 25-30 and column 2, lines 50-55).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Horne as taught by Ishibashi in order to transfer data from service providers over an unsecured environment that requires both low processing overhead, yet still prevents an unauthorized user from accessing the data.

Neither Horne nor Ishibashi explicitly disclose decrypting the control signals in accordance with the common key. However, Yokoyama discloses decrypting the control signals in accordance with the common key (column 13, lines 10-20).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Horne and Ishibashi by decrypting the encrypted control signals with the common key to generate decrypted control signals as taught by Yokoyama in order to minimize the necessity for storing and protecting a secret key for each receiver in the transmitting side.

6. As to claim 2, Horne discloses the semiconductor integrated circuit wherein the first decryption circuit and second decryption circuit are formed in a common circuit (column 2, lines 35-45, Horne teaches of forming common circuit by decrypting control signals and common key by the circuit, e.g., column 4, lines 28-36).

7. As to claim 3, Horne discloses the semiconductor integrated circuit wherein at least one of the first decryption circuit and the second decryption circuit comprises an AES circuit (column 4, lines 4-7).

8. As to claim 4, Horne discloses the semiconductor integrated circuit wherein the broadcast signal comprises a digital television signal and the processing unit comprises a DVB circuit (column 4, lines 21-27).

9. As to claim 5, Horne discloses the semiconductor integrated circuit wherein the input interface has a separate input for the encrypted common key connected to the decryption circuit (FIG. 2).

10. As to claim 6, Horne discloses the semiconductor integrated circuit wherein the secret key is unique to the semiconductor integrated circuit (column 4, lines 28-29).

11. As to claim 8, Horne discloses a television decoder comprising the semiconductor integrated circuit (column 2, lines 5-8 and lines 36-45).

12. As to claim 9, Horne discloses a system for broadcasting signals to a plurality of subscribers (column 2, lines 58-62) in which only authorized recipients are able to decrypt the broadcast signals (column 2, lines 60-68), comprising: a transmitter arranged to broadcast: signals (column 5, lines 59-65) encrypted according to control words (FIG. 4); a common key encrypted respectively according to a unique secret key of each authorized recipient (column 3, lines 65-68); and a plurality of receivers (column 1, lines 58-62), each comprising a semiconductor integrated circuit (column 2, lines 36-45), wherein the secret key is unique to each semiconductor integrated circuit (column 4, lines 28-30).

Neither Horne nor Ishibashi explicitly disclose control words encrypted according to a common key common to all authorized recipients. However, Yokoyama discloses control words encrypted according to a common key common to all authorized recipients (column 13, lines 1-6).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Horne and Ishibashi by control

words encrypted according to a common key common to all authorized recipients as taught by Yokoyama in order to minimize the necessity for storing and protecting a secret key for each receiver in the transmitting side.

13. As to claim 10, Horne disclose a device for decryption of broadcast signals (abstract), comprising: receiving a common key in encrypted form (column 4, lines 30-32); a secret key store configured to store a secret key (column 4, lines 28-30); a decryption unit comprising a first decryption circuit configured to receive encrypted control signals (column 2, lines 36-44 and column 3, lines 4-8) and a second decryption circuit configured to receive the common key in encrypted form and to decrypt the common key in accordance with a secret key from the secret key store (column 4, lines 28-36); and a processing unit configured to receive encrypted broadcast signals (column 2, lines 5-11) and decrypt the encrypted broadcast signals in accordance with the decrypted control signals received from the decryption unit (FIG. 4, FIG. 4, column 8, lines 42-58) and to provide decrypted broadcast signals to an output interface (column 2, lines 5-11); whereby the device is arranged such that the only route is to input the common key in encrypted form for decryption in accordance with the secret key (column 4, lines 28-36), and the only route to providing the control signals to the processing unit is to input them in encrypted form (FIG. 4, column 4, lines 34-36 and column 8, lines 42-58).

Horne doesn't explicitly disclose storing the common key in the common key store and decrypting the control signals in accordance with the common key. However,

Ishibashi discloses storing the common key in the common key store (column 6, lines 25-30 and column 2, lines 50-55).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Horne by storing common key in the common key store as taught by Ishibashi in order to transfer data from service providers over an unsecured environment that requires both low processing overhead, yet still prevents an unauthorized user from accessing the data.

Neither Horne nor Ishibashi explicitly disclose decrypting the control signals in accordance with the common key. However, Yokoyama discloses decrypting the control signals in accordance with the common key (column 13, lines 10-20).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Horne and Ishibashi by decrypting the encrypted control signals with the common key to generate decrypted control signals as taught by Yokoyama in order to minimize the necessity for storing and protecting a secret key for each receiver in the transmitting side.

14. As to claim 13, Horne discloses a method of decrypting encrypted broadcast signals (abstract), comprising: receiving encrypted broadcast signals (column 2, lines 5-11), encrypted control signals (column 3, lines 4-10 and column 4, lines 28-36), and encrypted common key signals at an input interface of a decryption unit formed on a semiconductor integrated circuit (column 4, lines 32-34, column 2, lines 5-11 and lines 36-69), the semiconductor integrated circuit comprising a processing unit (column 2,

lines 5-11); decrypting the encrypted common key utilizing a stored secret key to generate a common key (column 4, lines 28-36); providing the control signals to the processing unit (column 2, lines 5-11); and decrypting the encrypted broadcast signals in accordance with the control signals (FIG. 4, column 8, lines 42-58) and providing decrypted broadcast signals to an output interface of the decryption device (column 2, lines 5-11); whereby the circuit is arranged such that the only route is to input the common key in encrypted form for decryption in accordance with the secret key (column 4, lines 28-36), and the only route to providing the control signals to the processing unit is to input them in encrypted form (FIG. 4, column 4, lines 34-36 and column 8, lines 42-58).

Horne doesn't explicitly disclose placing common key in the common key store and decrypting the encrypted control signals with the common key to generate decrypted control signals. However, Ishibashi discloses placing common key in the common key store (column 6, lines 25-30 and column 2, lines 50-55).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Horne by placing common key in the common key store as taught by Ishibashi in order to transfer data from service providers over an unsecured environment that requires both low processing overhead, yet still prevents an unauthorized user from accessing the data.

Neither Horne nor Ishibashi explicitly disclose decrypting the encrypted control signals with the common key to generate decrypted control signals. However,

Yokoyama discloses decrypting the encrypted control signals with the common key to generate decrypted control signals (column 13, lines 10-20).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Horne and Ishibashi as taught by Yokoyama in order to minimize the necessity for storing and protecting a secret key for each receiver in the transmitting side.

15. As to claim 16, Horne discloses a method for broadcasting signals to a plurality of subscribers (column 2, lines 58-62) in which only authorized recipients are able to decrypt the broadcast signals (column 2, lines 60-68), the method comprising: encrypting control words and transmitting the encrypted control words (column 3, lines 4-8 and column 2, lines 1-11); encrypting a common key and transmitting the encrypted common key (column 3, lines 65-68 and column 4, lines 28-36); encrypting broadcast signals and transmitting the encrypted broadcast signals to the plurality of subscribers (column 1, lines 60-68 and column 2, lines 1-11); providing a secret key to each authorized recipient that is stored in a respective decryption unit (column 6, lines 5-10); receiving encrypted broadcast signals (column 2, lines 5-11), encrypted control signals (column 3, lines 4-10 and column 4, lines 28-36), and encrypted common key signals at an input interface of a decryption unit formed on a semiconductor integrated circuit, the semiconductor integrated circuit comprising a processing unit (column 4, lines 32-34 and column 2, lines 5-11); decrypting the encrypted common key utilizing a stored secret key to generate a common key (column 4, lines 28-36); providing the control

signals to the processing unit (column 4, lines 34-36 and column 8, lines 42-58) and decrypting the encrypted broadcast signals in accordance with the control signals (column 8, lines 42-58) and providing decrypted broadcast signals to an output interface of the decryption device (column 2, lines 5-11); whereby the semiconductor integrated circuit is arranged such that the only route is to input the common key in encrypted form for decryption in accordance with the secret key (column 4, lines 28-36), and the only route to providing the control signals to the processing unit is to input them in encrypted form (FIG. 4, column 4, lines 34-36 and column 8, lines 42-58).

Horne doesn't explicitly disclose decrypting the encrypted control signals with the common key to generate decrypted control signals and storing the common key in the common key store. However, Ishibashi discloses storing the common key in the common key store (column 6, lines 25-30 and column 2, lines 50-55).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Horne as taught by Ishibashi in order to transfer data from service providers over an unsecured environment that requires both low processing overhead, yet still prevents an unauthorized user from accessing the data.

Neither Horne nor Ishibashi explicitly disclose decrypting the encrypted control signals with the common key to generate decrypted control signals. However, Yokoyama discloses decrypting the encrypted control signals with the common key to generate decrypted control signals (column 13, lines 10-20).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Horne and Ishibashi as taught by Yokoyama in order to minimize the necessity for storing and protecting a secret key for each receiver in the transmitting side.

16. As to claim 19, Horne disclose a system for broadcasting signals to a plurality of subscribers (column 2, lines 58-62) in which only authorized recipients are able to decrypt the broadcast signals (column 2, lines 60-68), the system comprising: a transmitter configured to broadcast signals (column 5, lines 59-65) encrypted according to control words (FIG. 4), and a common key that is common to two or more authorized recipients, and a common key encrypted according to a secret key that is unique to each authorized recipient (column 3, lines 65-68); and a plurality of receivers configured to receive the broadcast signals (column 1, lines 58-62), each receiver comprising: receive a common key (column 4, lines 32-34, column 2, lines 5-11 and lines 36-69); a secret key store configured to store a secret key (column 4, lines 28-30).

A decryption unit comprising a first decryption circuit configured to receive encrypted control signals (column 2, lines 38-40 and lines 5-11) and a second decryption circuit configured to receive the common key in encrypted form (column 4, lines 28-36 and column 2, lines 36-45) and to decrypt the encrypted common key in accordance with a secret key from the secret key store (column 4, lines 28-36); and a processing unit configured to receive encrypted broadcast signals (column 4, lines 28-36 and column 2, lines 36-45) and decrypt the encrypted broadcast signals in

accordance with the decrypted control signals received from the decryption unit (FIG. 4, column 8, lines 42-58) and to provide decrypted broadcast signals to an output interface (column 2, lines 5-11); whereby the system is arranged such that the only route is to input the common key in encrypted form for decryption in accordance with the secret key (column 4, lines 28-36), and the only route to providing the control signals to the processing unit is to input them in encrypted form (FIG. 4, column 4, lines 34-36 and column 8, lines 42-58).

Horne doesn't explicitly disclose that control words are encrypted according to a common key that is common to all authorized recipients and to decrypt the encrypted control signals in accordance with a common key and to store the common key in the common key store.

However, Ishibashi discloses storing the common key in the common key store (column 6, lines 25-30 and column 2, lines 50-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Horne by storing the common key in the common key store as taught by Ishibashi in order to transfer data from service providers over an unsecured environment that requires both low processing overhead, yet still prevents an unauthorized user from accessing the data.

Neither Horne nor Ishibashi explicitly discloses that the control words are encrypted according to a common key that is common to all authorized recipients and to decrypt the encrypted control signals in accordance with a common key.

However, Yokoyama discloses that the control words are encrypted according to a common key that is common to all authorized recipients (column 13, lines 1-6) and to decrypt the encrypted control signals in accordance with a common key (column 13, lines 10-20).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Horne and Ishibashi by encrypting the control word according to a common key that is common to all authorized recipients and to decrypt the encrypted control signals in accordance with a common key as taught by Yokoyama in order to minimize the necessity for storing and protecting a secret key for each receiver in the transmitting side.

17. As to claims 12 and 21, Horne discloses the system wherein the decryption device is formed as a single semiconductor integrated circuit (column 2, lines 36-44) having an input interface for receipt of encrypted broadcast signals (column 2, lines 5-11 and lines 36-69), encrypted control signals (column 3, lines 4-10 and column 4, lines 28-36), and encrypted common keys (column 4, lines 32-34), and an output interface for output of decrypted broadcast signals (column 2, lines 5-11).

18. As to claims 7, 11 and 20, Horne doesn't explicitly disclose the common key store that is arranged to store multiple common keys. However, Ishibashi discloses the common key store that is arranged to store multiple common keys. (FIG. 9, item 110).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Horne by including the common key store that is arranged to store multiple common keys as taught by Ishibashi in order to increase security by including separate keys for each individual program.

19. As to claim 14, Horne disclose the method further comprising storing a secret key that is unique to the decryption unit in a secret key store in the decryption unit (column 4, lines 28-29).

20. As to claim 17, Horne discloses the method further comprising storing a secret key that is unique to the decryption unit in a secret key store in the decryption unit (column 4, lines 28-29).

21. As to claims 15 and 18, Horne doesn't explicitly disclose the method further comprising receiving multiple encrypted common keys, decrypting each of the encrypted common keys to generate multiple decrypted common keys, and storing the multiple decrypted common keys in a common key store in the decryption unit.

However, Ishibashi discloses the method further comprising receiving multiple encrypted common keys (column 6, lines 14-20, FIG. 9), decrypting each of the encrypted common keys to generate multiple decrypted common keys (column 6, lines

34-37), and storing the multiple decrypted common keys in a common key store in the decryption unit (FIG. 9, item 110, column 6, lines 25-30 and column 2, lines 50-55).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Horne by receiving multiple encrypted common keys, decrypting common keys and storing in the common key store as taught by Ishibashi in order to transfer data from service providers over an unsecured environment that requires both low processing overhead, yet still prevents an unauthorized user from accessing the data.

22. Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Response to Amendment

23. Applicant has amended claims 9-10, 13, 16 and 19. The amendments neither overcome the rejections nor necessitated citation of additional prior art references. See rejection above.

Response to Arguments

24. Applicant's arguments filed on 07/19/2007 have been fully considered but they are not persuasive for the reasons set forth below.

Applicant argues that: "More particularly, claim 1 specifies that 'the only route to placing a common key in the common key store is to input the common key in encrypted form for decryption in accordance with the secret key and the only route to providing the control signals to the processing unit is to input them in encrypted form for decryption in accordance with the common key'."

Examiner maintains that: Horne discloses whereby the circuit is arranged such that the only route is to input the common key in encrypted form for decryption in accordance with the secret key (column 4, lines 28-36, Horne teaches the concept by decrypting the received individual encrypted common key using the stored individual key), and the only route to providing the control signals to the processing unit is to input them in encrypted form (FIG. 4, column 4, lines 34-36 and column 8, lines 42-58, Horne teaches this concept by receiving control signals in an encrypted form). Ishibashi discloses placing common key in the common key store (e.g. see, column 6, lines 25-30 and column 2, lines 50-55). Yokoyama discloses decrypting the encrypted control signals with the common key to generate decrypted control signals (e.g. see, column 13, lines 10-20). In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642

F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Applicant argues that: "A second feature of the circuit defined in claim 1 is that all components are placed on the same integrated circuit, eliminating vulnerable interfaces that occur in previous smart-card based designs. For example, claim 1 specifies "a semiconductor integrated circuit...comprising ....". Home describes an encryption layering scheme, but Home is completely silent as to the precise circuit layout used. Therefore, this reference does not teach or suggest the central features recited in claim 1 wherein all components are provided on the same integrated circuit and providing secure routing of sensitive data (such as control signals and cryptographic keys) so that the data is not exposed at any vulnerable interface."

In response to applicant's arguments, the recitation "a semiconductor integrated circuit...comprising....." has not been given patentable weight because the recitation occurs in the preamble of claim 1. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Conclusion

25. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See accompanying discloser PTO 892.

- US 7,120,604 B2 – Maari discloses an integrated circuit comprising a key store and a processor, encoding and decoding unit.
- US 5,999,629 – Heer et al. discloses an integrated circuit comprising a key store and a processor unit.

26. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

27. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Suman Debnath whose telephone number is 571 270 1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SD

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER